Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Request Of The National Association Of State	)	RM-11780
911 Administrators To Address Issues Related	)	
To 911 Applications For Smartphones	)	

To: Chief, Public Safety and Homeland Security Bureau

COMMENTS OF
THE BOULDER REGIONAL EMERGENCY TELEPHONE SERVICE AUTHORITY

Joseph P. Benkert

Joseph P. Benkert, P.C.
8605 Porcupine Pointe
Parker, CO 80134-2786
(303) 948-2200

Its Attorney

February 2, 2017

Summary

The sheer number of potential 911-related smartphone "Apps" which have been and are likely to be developed, the practical requirement for App developers to create a distinct "look and feel" to their application for intellectual property protection purposes, the lack of knowledge or experience with 9-1-1 and public safety operations by many developers, the ability of Apps to create and send text-to-911 messages with "emergency information" including geographic coordinates or URLs for more information (which may be deleted, blocked or PSAPs may have policies against accessing for cybersecurity purposes), and their transmission of alarms directly to PSAPs without a commercial call center first clearing false alarms; all have the potential to overwhelm PSAPs with relevant and irrelevant information regarding actual incidents and false alarms. Apps may transmit to PSAPs medical or technical information which dispatchers cannot be expected to have the expertise to interpret and use. The ability of App developers to churn out Apps which users can utilize to send text-to-911 messages and attachments to PSAPs, and/or program to automatically send text-to-911 messages to PSAPs, can overwhelm a PSAP with frivolous calls-for-assistance and irrelevant information. In short, 911-related Apps have the potential to turn the nation's effective 9-1-1 and Emergency Response Systems into a Tower of Babble, and waste limited resources of PSAPs and First Responders dealing with frivolous calls and false alarms.

This potential is exacerbated by the fact that Apps transmitting messages to 9-1-1 by text-message require no prior input, approval, consent of the PSAP or even notice to the PSAP. Such Apps require no ongoing "backroom support" of the App provider for the PSAP. PSAPs may not even be aware an App exists before receiving a message from the App, and may not have knowledge of the App provider or the App provider's contact information in the event a problem

is experienced with an App. Indeed, Apps could be sold or distributed for free with malfunctioning or non-existent user-location and call-routing functionality, and PSAPs may not have any means of identifying or notifying the developer of the errors.

Not only can App developers increase the burdens and costs to PSAPs, delay responses to real emergencies, and render text-to-911 messages so unreliable as to make text-to-911 service unusable for anyone; it has been demonstrated that some App providers will misrepresent approval by 9-1-1 stakeholders, misrepresent the reliability of CMRS and broadband/VoIP providers and devices to connect to the correct PSAP, and otherwise mislead consumers in order to advance their own pecuniary interest.

A four-part solution is required. The first part of the solution is for the FCC to adopt regulations requiring CMRS service and device providers to publish their location APIs so that any voice, text or data application for 9-1-1 can access the more accurate data the CMRS providers have agreed to provide under their "Roadmap" and "Parallel Path" commitments. Second, the Commission should establish a "Standards Authority" to (i) establish standards for 9-1-1 related Apps (such as the inability of users to modify location data transmitted to the 9-1-1 system, the transmission of useful information with XML tags so that CAD and other PSAP systems can display information from different Apps in a uniform format for dispatchers, and automated alarms will first be transmitted to a commercial call center for clearing of false alarms, for example), (ii) review and approve Apps which meet the standards, (iii) assign reference numbers and codes to be used in the protocols of messages transmitted by approved Apps identifying to the 9-1-1 system that an App is approved and messages from it should be accepted, and (iv) publish a list of approved Apps to assist consumers. The third part of the solution is for the Commission to adopt regulations prohibiting service providers and 9-1-1

system providers from accepting data from unapproved 911-related Apps, and prohibiting CMRS and device providers from including in their App stores unapproved 911-related Apps. (Insofar as the Commission requires or may require interconnected text-messaging and VoIP applications to provide 9-1-1 messaging and calling capability, approval of their 9-1-1 functionality by the Standards Authority would also be required.)

Finally, certain statutes and regulations would be required, and the Standards Authority should identify and propose the specific statutes required. Generally, statutes and regulations would be required prohibiting App developers from falsely representing their approval by the Standards Authority, and from falsely representing approval of any 9-1-1 stakeholder including state and local 9-1-1 Authorities, state or federal regulatory agencies or stakeholder associations. Statutes and regulations would be required prohibiting an *unapproved* App from spoofing or otherwise using protocols assigned by the Standards Authority to an *approved* App to gain access to the 9-1-1 System. The statutes must also provide criminal penalties for violations, because (i) the harm that could result to users from violations and the impact of unapproved Apps on the 9-1-1 system is substantial, and (ii) the minimal capital investment to develop Apps means that violators could be "judgment proof," limiting the deterrent effect of potential civil liability.

Table of Contents

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Request Of The National Association Of State 911 Administrators To Address Issues Related To 911 Applications For Smartphones	)	RM-11780
	)	
	)	

To: Chief, Public Safety and Homeland Security Bureau

COMMENTS OF
THE BOULDER REGIONAL EMERGENCY TELEPHONE SERVICE AUTHORITY

The Boulder Regional Emergency Telephone Service Authority ("BRETSA"), by its attorney, hereby submits its comments on the October 18, 2016 request of the National Association of State 911 Administrators ("NASNA") for the Commission to address issues related to 911 applications for smartphones ("Request").[1]

I. BRETSA Shares NASNA's Concerns With 9-1-1 Smartphone Apps.

BRETSA has previously raised concerns with 9-1-1 related smartphone applications ("Apps") in a number of proceedings.[2] While BRETSA believes that the Apps and application-

[1] BRETSA is a Colorado 9-1-1 Authority which establishes, collects and distributes the Colorado Emergency Telephone Surcharge to fund 9-1-1 service in Boulder County, Colorado.

[2] *See* Joint Comments of the Boulder Regional Emergency Telephone Service Authority And The Colorado 9-1-1 Task Force, filed December 12, 2011 in PS Docket Nos. 11-153, *In the Matter of Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications*, and 10-255, *In the Matter of Framework for Next Generation 911 Deployment*, at 35-41 ("Joint Comments of BRETSA And The Colorado 9-1-1 Task Force, filed December 12, 2011 in PS Docket Nos. 11-153 and 10-255")(Available at https://www.fcc.gov/ecfs/filing/6016877846/document/7021750354); Reply Comments of the Boulder Regional Emergency Telephone Service Authority, filed January 14, 2013 in PS Docket Nos. 12-333, *In the Matter of Legal and Statutory Framework for Next Generation 9-1-1 Services*, 11-153 and 10-255, at 14-15 ("BRETSA January 14, 2013 Reply Comments in PS Docket Nos. 12-333, 11-153 and 10-255")(Available at https://www.fcc.gov/ecfs/filing/6017158015/document/7022104509); Comments of The Boulder Regional Emergency Telephone Service Authority On Policy Statement And Second Further Notice Of Proposed Rulemaking Regarding Text To 9-1-1, filed April 4, 2014 in PS Docket Nos. 11-153 and 10-255, at 13-25 ("BRETSA April 4, 2014 Comments in PS Docket Nos. 11-153 and 10-255") (Available at https://www.fcc.gov/ecfs/filing/6017611014/document/7521096988); Comments of the Boulder Regional Emergency Telephone Service Authority, filed July 15, 2014 in GN Docket No. 14-28, *In the Matter of Protecting and Promoting the Open Internet*, at 12-15 ("BRETSA, July 15, 2014 Comments in GN Docket No. 14-

driven services can enhance the capabilities of 9-1-1 and the public safety, (i) the sheer number of Apps being developed and likely to be developed, (ii) the development of Apps by parties with little or no knowledge of public safety operations, (iii) the development and marketing of some Apps by thinly capitalized parties, and (iv) the development of multiple Apps with the same or similar functionality but each with a different "look and feel" for purposes of intellectual property protection; can interfere with the effective delivery of 9-1-1 calls and messages and the timely dispatch of First Responders, and potentially defraud the public.[3] Indeed, the proliferation of 9-1-1 related Apps threatens to turn 9-1-1 Service into a tower of babble, and leave consumers confused as to how to best get help when they need it most.

II. NASNA And BRETSA Have Identified Substantive Concerns With 911-Related Smartphone Apps.

BRETSA believes that the majority of parties developing 911-related smartphone Apps, are doing so out of a *bona fide* desire to improve public safety and emergency response. However 9-1-1 stakeholders are already identifying issues with many of these Apps, and with the sheer number of Apps which are and will be available. Among the identified and potential issues are:

- Inaccuracy of location data, including user-ability to "spoof" location data. Request, at 1, 2.
- Inability of PSAP to "re-bid" user (device) location. Request, at 1.
- "9-1-1 Call Buttons" facilitating "pocket dials". Request, at 2.

28")(Available at https://www.fcc.gov/ecfs/filing/6018000919/document/7521496081); and Comments of the Boulder Regional Emergency Telephone Service Authority on Policy Statement and Notice of Proposed Rulemaking, filed March 23, 2015 in PS Docket Nos. 14-193, *In the Matter of 911 Governance and Accountability*, and 13-75, *In the Matter of Improving 911 Reliability*, fn 14 at 27 ("BRETSA March 23, 2015 Comments un PS Docket Nos. 14-193 and 13-75")(Available at https://www.fcc.gov/ecfs/filing/60001027340/document/60001041288).

[3] It is not merely the sale of ineffective Apps or misleading claims about 9-1-1 related Apps that is of concern, but the consequences to individuals who rely on such Apps to contact 9-1-1 in an emergency, which will harm the public.

- Automatic generation of duplicate 9-1-1 messages, such as having the smartphone automatically generate a text-to-911 message when the user places a voice call to 9-1-1. Request, at 2.

- Automatic insertion of location information in the body of a text-to-911 message, that could be viewed as a malicious link.[4] Request, at 2.

- Embedding the URL of a website or webpage providing supplemental information regarding the user or incident in a text message, which could be viewed as a malicious link or which could pose a cybersecurity threat. *See, e.g.*, Request, at 2.

- Automatic transmission of a pre-recorded message which may go on too long or indefinitely. Request, at 2.

- Automatic transmission of data or a message pre-selected by the user, unless the user affirmatively cancels the transmission prior to the time the user scheduled the information to be transmitted.

- Transmission of automated alarms to PSAPs without a commercial call-center first clearing false alarms.[5]

- Transmission of technical or medical data to PSAPs which dispatchers are not trained or qualified and cannot be expected to interpret, without trained and qualified personnel in a commercial call center first reviewing and interpreting the data.[6]

- Transmission of data to PSAPs without XML or other tagging or coding of data for display in a common format developed by the PSAP CAD vendor.[7]

---

[4] Note that the ability of an App to transmit App-generated or user-selected information in a text-to-911 message means that even well-meaning developers can develop and market Apps to the public without any prior consultation or coordination with public safety officials or PSAPs.

[5] BRETSA March 23, 2015 Comments in PS Docket Nos. 14-193 and 13-75, fn 14 at 27 (Available at https://www.fcc.gov/ecfs/filing/60001027340/document/60001041288); BRETSA, July 15, 2014 Comments in GN Docket No. 14-28, at 13 (Available at https://www.fcc.gov/ecfs/filing/6018000919/document/7521496081); BRETSA April 4, 2014 Comments in PS Docket Nos. 11-153 and 10-255, at 17 (Available at https://www.fcc.gov/ecfs/filing/6017611014/document/7521096988); Joint Comments of BRETSA and The Colorado 9-1-1 Task Force, filed December 12, 2011 in PS Docket Nos. 11-153 and 10-255, at 35, 37-38, 41 (Available at https://www.fcc.gov/ecfs/filing/6016877846/document/7021750354).

[6] BRETSA March 23, 2015 Comments in PS Docket Nos. 14-193 and 13-75, fn 14 at 27 (Available at https://www.fcc.gov/ecfs/filing/60001027340/document/60001041288); BRETSA, July 15, 2014 Comments in GN Docket No. 14-28 at 13,14 (Available at https://www.fcc.gov/ecfs/filing/6018000919/document/7521496081); BRETSA April 4, 2014 Comments in PS Docket Nos. 11-153 and 10-255, at 17 (Available at https://www.fcc.gov/ecfs/filing/6017611014/document/7521096988); Joint Comments of BRETSA And The Colorado 9-1-1 Task Force, filed December 12, 2011 in PS Docket Nos. 11-153 and 10-255, at 35, 37-38 (Available at https://www.fcc.gov/ecfs/filing/6016877846/document/7021750354).

[7] BRETSA March 23, 2015 Comments in PS Docket Nos. 14-193 and 13-75, fn 14 at 27 (Available at https://www.fcc.gov/ecfs/filing/60001027340/document/60001041288); BRETSA, July 15, 2014 Comments in GN Docket No. 14-28, at 13,14 (Available at https://www.fcc.gov/ecfs/filing/6018000919/document/7521496081); BRETSA April 4, 2014 Comments in PS Docket Nos. 11-153 and 10-255, at 17-18 (Available at

- Transmission to the PSAP of information irrelevant to Emergency Response.[8]
- App provider misrepresentation of the endorsement of their Apps by regulatory agencies, public safety associations or authorities, and misrepresentation of the capabilities of Apps and other telecommunications services and technologies for communicating with PSAPs. Request, at 1.
- Direct access to CAD and other PSAP systems and data therein by Apps.

As BRETSA has stated, the primary task of a 9-1-1 dispatcher/calltaker is and will continue to be to determine the nature and location of an emergency, and use PSAP systems to dispatch the appropriate First Responders who can arrive at the scene of the emergency the soonest and render the assistance required. This is not to minimize the tasks or job requirements of public safety dispatchers. Indeed, this primary dispatcher function requires specific communications skills, expertise in multiple PSAP systems, and working knowledge of state and local codes and PSAP- and First Responder agency-business rules. For a more thorough discussion of the unique, relatively rare and important skill-set required of dispatchers, s*ee* Comments of the Boulder Regional Emergency Telephone Service Authority, filed July 22, 2016 in CG Docket No. 16-145, *Transition from TTY to Real-Time Text Technology*, and GN Docket No. 15-178, *Petition For Rulemaking To Update The Commission's Rules For Access To Support The Transition From TTY To Real-Time Text Technology, And Petition For Waiver Of Rules Requiring Support Of TTY Technology*, at 11-20 ("BRETSA July 22, 2016 Comments in CG Docket No. 16-145, and GN Docket No. 15-178")(Available at https://ecfsapi.fcc.gov/file/10722185086488/BRETSA%20Comments%20CG%2016-145%20RTT%20GN%2015-178%20filed%20160722.pdf). *See, also*, BRETSA, July 15, 2014 Comments in GN Docket No. 14-28, at 13 (Available at

https://www.fcc.gov/ecfs/filing/6017611014/document/7521096988); BRETSA January 14, 2013 Reply Comments in PS Docket Nos. 12-333, 11-153 and 10-255, at 15 (Available at https://www.fcc.gov/ecfs/filing/6017158015/document/7022104509).

[8] BRETSA, July 15, 2014 Comments in GN Docket No. 14-28, at i, 14 (Available at https://www.fcc.gov/ecfs/filing/6018000919/document/7521496081).

https://www.fcc.gov/ecfs/filing/6018000919/document/7521496081); and BRETSA April 4, 2014 Comments in PS Docket Nos. 11-153 and 10-255, at 20 (Available at https://www.fcc.gov/ecfs/filing/6017611014/document/7521096988).

Simply put, the task performed by Dispatchers which will have the most positive impact on outcomes in the greatest percentage of incidents is the expeditious determination of the nature and location of the incident, so they can dispatch appropriate resources to minimize the response time (the time which elapses between receipt of the "9-1-1 call" and arrival at the scene of the incident of First Responders appropriate to the type of incident.) While certain additional information may be required depending on the type of incident, and additional data may be useful for subsequent investigation; the provision by Apps of irrelevant information in varying and unique formats can only complicate this primary task and *delay* Emergency Response.[9]

III. Practical Requirements for 911-Related Smartphone Apps.

BRETSA has identified practical requirements for Apps which, along with measures identified by NASNA, will best assure that they contribute positively to emergency response and public safety. BRETSA will discuss at Section IV below the organization ("Standards Authority") and process to implement these measures.

A. CMRS Providers And Device Makers Must Make Their Location APIs Available to App Developers.

As BRETSA stated in BRETSA's April 4, 2014 Comments in PS Docket Nos. 11-153 and 10-255, at 16-18, 21-25 (Available at https://www.fcc.gov/ecfs/filing/6017611014/document/7521096988), CMRS providers and

[9] Because of the specific and relatively rare skillset required of dispatchers, and the high-stress/high-turnover nature of the job, many PSAPs are continually recruiting, hiring and training new dispatchers. Generally, only one-to-two percent of job applicants will be found qualified for dispatch positions, and about one-half of those hired resign prior to completing training. Thus, we must not add new qualifications to the job requirements for dispatchers. We should be seeking technological solutions, procedures and requirements to lessen rather than increase the burdens on public safety dispatchers.

device manufacturers should be required to publish their location APIs for their native location applications or functions, so that VoIP, text-to-911 and other Apps can utilize the devices' native location data. Both the national and non-national CMRS providers have committed to improve the accuracy of location data pursuant to the "Roadmap" and "Parallel Path" commitments in PS Docket No. 07-114. *See* Wireless E911 Location Accuracy Requirements, Fourth Report and Order, 30 FCC Rcd 1259, 1267-1273 (2015) (Available at https://www.fcc.gov/ecfs/filing/60001013505/document/60001025925, para. 22-40. Apps should also be able to access native device communications functionalities as necessary to permit rebidding for updated location data.

CMRS providers will likely adopt any new location methods or technologies in order to meet FCC location accuracy requirements, assuring that Apps accessing this location information will provide the 9-1-1 system the most accurate location information for call-routing, and PSAPs the most accurate location information for Emergency Response. However in the event more accurate location technologies and/or location technologies with faster times-to-first-fix, or alternative accurate location technologies are developed which are not adopted by CMRS providers, App providers should be permitted to use them upon reasonable demonstration of their accuracy to the Standards Authority discussed at Section IV below.

Location information must be transmitted in a standardized format and method, (i) to enable accurate call routing, (ii) avoid the data being viewed as a malicious link and/or cybersecurity risk and deleted, (iii) assure PSAPs can access and use the data and (iv) PSAP systems can automatically and efficiently identify caller locations. It is also critical that location information not be subject to modification by users, which would permit location spoofing, swatting, and other malicious or frivolous use of the 9-1-1 and Emergency Response systems.

B. Certain Apps Must Deliver Calls Or Messages To Commercial (Non-PSAP) Call Centers Rather Than Directly To PSAPs.

There are a number of Apps which cannot be permitted to deliver calls or messages *directly* to PSAPs, because of their potentially disruptive effect, because they would supply data PSAP personnel are not trained or experienced in interpreting, or because they are likely to generate a high percentage of "false alarms."

1. One-Button 9-1-1 Functionality.

The concern with one-button 9-1-1 functionality is that, as with the programming of the number 9 button on a CMRS device to dial 9-1-1 when depressed, they are prone to "pocket dialing" and false 9-1-1 calls. Thus, as with automated premises alarms, any App providing one-button 9-1-1 functionality should be required to transmit calls or messages to a commercial call center, for clearing of false alarms and relaying of legitimate alarms to the appropriate PSAP.

BRETSA can anticipate the Standards Authority discussed at Section IV hereof approving one-button 9-1-1 functionality if an App developer can demonstrate that its particular App would not result in false alarms. This might include situations where (i) the one-button 9-1-1 functionality is disabled by default, (ii) the user must enter a specific sequence of commands or numbers on the user-device to activate the one-button 9-1-1 functionality, and (iii) the one-button 9-1-1 functionality would be disabled after a certain interval unless the user pressed a key to extend the period of activation. This would allow a user to enable the one-button functionality if it would give them comfort while walking to their car on a dark street late at night, for example, but the functionality would "time-out" after a reasonable period of time to reduce the opportunity for "pocket dialing" 9-1-1. Approval of such a waiver application would be discretionary with the Standards Authority, however.

2. Automated Transmission Of Alarms, Or Other User-Selected Data, To 9-1-1.

Just as with automated premises alarms, Apps which automatically send alarms, messages or user-selected data to 9-1-1 have the potential to generate a high-number of false alarms.[10] With automated premises alarms, many or most jurisdictions (i) require alarm system activations to be screened by a commercial call center to clear false alarms when possible, (ii) require PSAPs answer alarm calls on a secondary basis, (iii) require PSAPs dispatch officers in response to alarm calls on a secondary, as-available basis, and (iv) charge a fee to residents who have monitored alarm systems and/or charge a fee for responses to false alarms; all because of the high percentage of false alarms. Because automated alarms and transmission of messages or data from Apps to 9-1-1 will have an equal or even greater potential for transmission of false alarms to PSAPs, false alarms cleared and relevant information identified for relay to the appropriate PSAP.

Included within this category of App are those which would provide for a user to create and schedule a message in the App or user's device, in the App provider's systems or "in the cloud" for transmission to 9-1-1 at a later date or time, unless the user takes *affirmative* action to cancel the message before it is sent. Calls to 9-1-1 which are not made in real time concerning a currently occurring incident, are generally *misuses* of 9-1-1, and can prevent calls concerning real, current emergencies from going through. Pre-scheduled messages to 9-1-1 which are sent automatically *unless there is affirmative intervention by the user*, rather than the user having to take an affirmative action *to send* the message, are even less likely to concern an actual, current, emergency. When the user creates and queues such a message, the user is speculating that some

[10] It is the automated transmission of information to the PSAP, and is not a live call, rather than the fact that the user may select the data to transmit, which requires review by a commercial call center prior to forwarding to the PSAP. Automated transmissions intended for a PSAP must be reviewed by a commercial call center whether the content is automatically generated or generated by the user.

emergency *may* occur which would prevent the user from cancelling the message, or that the only reason the user would not cancel the transmission is if some harm befell the user. However it is *more* likely that a user would not cancel the transmission of such a message because the user forgot to cancel it, the battery in the user's device died or some similarly benign reason. Where a message to 9-1-1 is queued in a remote system "or the cloud" for transmission at some future time, location information necessary for call routing may not be current.

3 Technical, Health Monitoring Or Other Medical Data.

Apps which transmit technical or medical data such as crash telemetry, or real-time health data such as automatically monitored blood sugar levels for diabetics, for example, should not transmit the data directly to PSAPs. PSAP personnel are not trained or experienced to analyze and interpret this data, and it is unreasonable to expect PSAP personnel to be able to interpret data from the variety of technical and medical disciplines which such Apps might present. It should be remembered that the Commission has found that eighty percent of PSAPs have only between one and five dispatch positions.[11]

Technical and medical data must be first sent to commercial call centers, staffed with personnel trained to interpret technical or health data.[12] The commercial call processing centers would clear false alarms (caused by malfunctioning equipment or user error), or interpret the technical or health data so as to forward usable information to the appropriate PSAP via the NG9-1-1 system. "Interpreting the data so as to be usable" would mean, for example, (i)

[11] Public Safety and Homeland Security Bureau, "A Next Generation 911 Cost Study: A Basis for Public Funding Essential to Bringing a Nationwide Next Generation 911 Network to America's Communications Users and First Responders," White Paper (Sept. 2011) available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-309744A1.pdf , at 13.

[12] Whether automated systems for clearing alarms or interpreting data (such as translating crash telemetry data into a color-coded crash-severity index) would be permitted, would be determined on a case-by-case or App-by-App basis by the Standards Authority as discussed in Section IV below. Translating crash telemetry data into a color-coded crash-severity index could lead to confusion unless *all* such Apps use a common or standard color-coded crash-severity index.

describing to the dispatcher the likely condition of the end user such as "likely disoriented," "probably immobile," "likely unconscious," (ii) the approximate time within which the end user needs to be located and receive treatment to avoid death or permanent injury, and (iii) the appropriate First Aid treatment according to standard protocols. Raw technical or medical data might also be provided the PSAP, *along with* the more practical information for Emergency Response purposes, for the PSAP to relay to the hospital to which the end user will be transported.

BRETSA notes that in the case of an App associated with a health-monitoring device, such as blood sugar levels for a diabetic, the App may report blood sugar levels which are a cause for concern and action to the commercial call center *prior* to the situation reaching a critical or emergency status. Personnel at the commercial call center might then contact the end user directly and advise of actions the user should take to remedy the situation and avert the situation reaching an emergency status. Providing for call-center receipt and interpretation of the monitoring data rather than transmitting the data directly to the PSAP would thus be consistent with best practices in any event. PSAPs lack the capacity and expertise to provide such remedial advice to end users prior to their situation reaching an emergency status, and App providers should not leverage taxpayer- and ratepayer-supported PSAPs in such a manner for their own pecuniary benefit.

C. Transmission Of "Duplicate" Messages.

NASNA has identified an App functionality in which a text message would be automatically transmitted to 9-1-1 whenever the user dialed 9-1-1. The problem with this type of application is that the messages arriving in different formats may not be identified as being transmitted by the same user with respect to the same incident. The duplicate messages could

needlessly tie up PSAP personnel and resources, without any commensurate benefit. While the prospect of such a duplicate message may not seem burdensome in the abstract; it must be remembered that PSAPs handle many calls, as well as conducting dispatch operations. A single incident may generate multiple 9-1-1 calls from different users, and in fact accidents on busy highways have been known to cause over 100 9-1-1 calls. Apps generating 100 text messages in addition to 100 voice calls concerning such a highway accident would further overwhelm PSAPs and further inhibit PSAPs from responding to other incidents.

However a prohibition on transmission of duplicate messages to the PSAP as described by NASNA need not necessarily preclude all 9-1-1 transmissions by alternative paths. In the wake of the April 2014 multistate 9-1-1 outage, a number of jurisdictions sought ANI and ALI data for individuals who had called 9-1-1 but whose calls had not gotten through due to the outage.[13] Where such ANI and ALI data was provided, it was provided after some delay, limiting the effectiveness of First Responders following up with respect to the incidents the callers wished to report.[14] If a means were developed whereby each time a user called 9-1-1, ANI and ALI data for the call was transmitted to the appropriate PSAP via an alternative transmission path, PSAP systems could be programmed to compare the ANI data for calls received over the primary transmission paths and alternative transmission path, and display ANI and ALI information received over the alternative path *not* matched with a 9-1-1 call received within a given period and having a minimum duration. This would identify to PSAPs in real time calls to

[13] *See* Letter of June 3, 2014 from Stephanie Fritts, 9-1-1 & Emergency Management Director, Pacific County, Washington, to Marlene H. Dortch, Secretary, FCC at 2 (Available at https://www.fcc.gov/ecfs/filing/6017713191/document/7521202054); Letter of July 2, 2014 from James Quackenbush, Thurston 9-1-1 Communications Executive Director, Thurston County, Washington to Marlene H. Dortch, Secretary, FCC at 2 ("Available at https://www.fcc.gov/ecfs/filing/6017870784/document/7521364865"), and Comments of the Washington State E9-1-1 Coordination Office in PS Docket No. 14-72, *Inquiry into Circumstances of Major 911 Outage Centered in Washington State on April 9-10 , 2014*, at 5 ("Available at https://www.fcc.gov/ecfs/filing/6017863206/document/7521356395").

[14] Id.

9-1-1 which had not been completed and answered on *an ongoing basis*, and not just during an outage. PSAP systems might even be developed with the functionality to automatically transmit standard text messages to those users from which a call was not received over the primary path; and inquiring as to the whether the user intended to contact 9-1-1 and require assistance.

Moreover, during a 9-1-1 outage, First Responders could be dispatched to caller locations based upon the ANI/ALI data transmitted via the alternative path. Each PSAP or jurisdiction could determine if it wished to use these functionalities and the manner in which it wished to use them. However without a Standards Authority to assess whether there was sufficient utility in and demand for such functionalities and coordinate their development, the functionalities will not likely be developed due to the number of entities which must cooperate in their development (e.g., originating service providers, NG9-1-1 providers (SSPs), 9-1-1 telephone system providers, and/or CAD system providers).

D. Transmission of Supplemental Data To PSAPs.

Applications and services are currently available which are intended to provide supplemental data (including multimedia data) regarding the end user, premises or incident to a PSAP when the end user calls or texts 9-1-1. Some of these Apps or services require a server in the PSAP and the PSAP purchase or subscribe to software from the App or service provider. Others embed a URL in a text-to-911 message with the expectation that the dispatcher will click on the link to access the website or webpage to access the additional information. This link may be deleted or the message blocked by firewalls, or PSAP policy may prohibit dispatchers from clicking on such links. Security and technical considerations may also prevent data from such websites or webpages from being automatically entered into the CAD incident record.

As NG9-1-1 is deployed, the opportunities will increase for Apps to transmit supplemental data directly to PSAPs, and for centralized databases to reside on the ESInet. The cybersecurity risks presented by such supplemental data and databases will also increase. Thus, for an App to be approved by the Standards Authority, the App provider must implement cybersecurity measures, depending on how it provides data to PSAPs, and transmit the data in a standard manner and format. *See* Section E below.

Apps should also be required to limit the categories of supplemental data to that which the Standards Authority approves,15 and require end users to update or affirmatively confirm the continuing accuracy of data at specified intervals; or delete the records. The categories of data and intervals within which data must be updated or confirmed would be as specified by the Standards Authority, discussed at Section IV below. Data which is wholly irrelevant to any Emergency Response, when viewed from the perspective of trained and experienced Dispatchers and First Responders, can only be a distraction and delay Emergency Response. Information which is no longer accurate can be worse than no data at all, as it can result in First Responders responding to the wrong location, looking for the wrong person, can place First Responders at risk, etc.

E. Transmission Of Data To PSAPs Without XML Or Other Tagging Or Coding.

There are already numerous Apps being developed which will transmit data to a PSAP, or transmit a URL from which data can be retrieved. Apps which are successful in the marketplace will generate numerous copy-cat Apps which provide the same functionality, but with each such App having a unique "look and feel" for purposes of intellectual property

[15] As discussed below, individuals with PSAP and First Responder operational experience should be included in the Standards Committee membership, who can identify information which will in-fact assist with expeditious dispatch and emergency response, and that information which will not advance those ends.

protection. A result of creating a unique look and feel for each App is that it will result in data elements being placed at different locations on the screen, and formatted differently, potentially delaying dispatchers in locating relevant data.

If permitted data elements are tagged or coded by type, then (i) App developers can design whatever interface they believe will best serve the user market they intend to serve, and best protect their intellectual property rights, and (ii) CAD and other PSAP system suppliers can design a single display format for their PSAP customers which would be consistent across all App-data sources, and also consistent with the look and feel of the CAD system screens generally. This would allow a dispatcher to find the same data in the same place on the CAD screen, no matter what App the end user is using. This will reduce the time required for dispatchers to access the information they require, and improve efficiency of PSAP operations.

F. Apps Should Be Denied Direct Access To CAD And Other PSAP Systems And Data.

There are new types of Apps which are intended to access and distribute to the public information resident in PSAP systems. These Apps can provide public safety benefits, such as crowd-sourced response to specific type of emergencies.

BRETSA isolates its CAD system from the Internet and other networks, in order to protect the system and to protect CAD data from unauthorized disclosure. Even the agencies which own the data regarding incidents in their jurisdictions and to which they responded, do not access their CAD data directly on the CAD system. A contractor engaged by BRETSA writes interfaces which identify data belonging to each agency, pushes that data in real time to a server dedicated to the agency ("Reporting Server"), and maps the data to the agency's data management system's data structure.

BRETSA recently proposed to allow one of these new types of Apps to access permitted data through such a Reporting Server, for dissemination to the public. However the App provider declined, and declined even to test BRETSA's reporting server architecture which limited the data available to the App to that it purported to need and which it was permitted to access. The App provider stated that in every other jurisdiction in which it disseminates certain CAD data to the public, it accesses the data directly on the PSAP CAD systems.

It is clear that standards are also required for these new types of Apps, which are intended to access data contained within PSAP systems and make it available to the public. Such standards must provide for the Apps to access only that data which they are authorized to access and publish, that the App provider is CJIS certified if it will be access law data, and that it will suppress data which it accesses but is not authorized to publish, or which state or local law or agency policy prohibits from publication. The standards must assure that CAD systems and the integrity of the data in those systems is protected, chain of evidence is not compromised, cyber threats are not introduced into PSAP systems, and data which is prohibited by law from being released to the public is not released.[16] It would be appropriate for the Standards Authority to address standards for these types of Apps and approve standards-compliant Apps, as well as those types of Apps which transmit data *to* PSAPs. Standards Authority approval of these Apps would ease the burden on PSAPs of vetting such Apps.

G. Other Matters.

Several years ago, a speaker at a Colorado 9-1-1 Task Force Meeting described a functionality of NG9-1-1 which would communicate to the NG9-1-1 System and PSAP if the

[16] Where a party requests agency data pursuant to open records laws, the responsible agency has the opportunity to review the data and deny production of documents including data excepted under the open records laws, or which the agency is legally prohibited from disclosing. Where a party is requesting real-time electronic access to PSAP data as it is being created, reasonable measures are required to protect the integrity of PSAP systems and data, and avoid disclosure of information not subject to or prohibited from disclosure.

profile the caller had set-up in his or her device indicated a language preference other than English (or, presumably, the profile indicated the caller was deaf or hard-of-hearing). This would allow the NG9-1-1 or PSAP systems to conference-in an appropriate interpreter *during call set-up*, rather than requiring a dispatcher to recognize that the person was not speaking English, conference in an interpreter service, have that service determine the language the caller was speaking, and get the correct interpreter on the line. It would allow the interpreter to be conferenced in within seconds rather than minutes. Such a reduction in the time required for the dispatcher to be able to communicate with the caller could have a significant impact on the effectiveness of emergency response.

In the case of callers who are deaf or hard-of-hearing, Relay Services do not have the technical capabilities to quickly and efficiently identify the caller's location and responsible PSAP to which the Relay Service should connect and relay the caller's emergency.[17] Dispatchers are not generally hired for proficiency in the various sign-language dialects necessary to communicate with by sign language with an excited caller, who may be using cell-phone video. It is hard enough for PSAPs to hire and retain dispatchers with the necessary skills without adding such sign-language skills to the necessary qualifications. Given the relatively small number of 9-1-1 calls many PSAPs receive from deaf and hard-of-hearing individuals, it would be difficult for dispatchers to maintain such proficiency. However, providing for deaf and hard-of-hearing individuals *to dial 9-1-1 directly*, and have *the 9-1-1 system* route the call to the correct PSAP *and* establish the connection with the Relay Service, would allow the call to be routed to the correct PSAP and connect to a Relay Service in seconds, rather than the minutes

[17] In Comments filed in PS Docket No. 11-153, Krystallo Tziallila, a deaf woman, described her attempt to reach 9-1-1 through a Relay Service after being involved in an auto accident, and the Relay Service CA's inability to determine her location, determine the PSAP serving her location and to connect the call to that PSAP. See December 14, 2011 Informal Comments of Krystallo Tziallila in PS Docket No. 11-153 (available at https://ecfsapi.fcc.gov/file/7021750686.pdf).

required for a Relay Service to identify the correct PSAP to receive the call and connect to the PSAP.

That is, in an NG9-1-1 environment, in an emergency, a deaf or hard-of-hearing end-user would *not* dial 7-1-1 to connect to a Relay Service, which *lacks* the capabilities to efficiently identify the correct PSAP to receive the call, and connect the call to that PSAP. Instead, the end-user would call 9-1-1 and the 9-1-1 system would conference in a Relay Service. (Only the PSAP serving the area in which the caller is located can dispatch First Responders to the caller's location, but a Relay Service CA can be located anywhere and assist the end user in communicating with the PSAP.) The 9-1-1 system could even route the call to a CA trained or experienced in assisting with 9-1-1 calls, if available.

These and other functionalities which can take advantage of the IP nature of NG9-1-1 to improve Emergency Response, can only be developed through cooperation among device manufacturers, originating service providers, NG9-1-1 Service Providers and the 9-1-1 Community, including individuals with operational experience in PSAPs. The Standards Authority discussed in Section IV should include representatives of such parties. This type of functionality should be referred to the Standards Authority to consider, and coordinate their development and deployment.

IV. Adoption and Enforcement of Standards.

It is easy to articulate standards which 911-related Apps should follow. Enforcement of standards for smartphone Apps presents quite another challenge. However in the case of 911-related Apps in a legacy E9-1-1 environment, messages to PSAPs must transmit text messages to PSAPs via TCC (sometimes including a URL for access to additional data), or utilize a server installed at a PSAP. In an NG9-1-1 environment, Apps would transmit data to PSAPs via TCC or

NG9-1-1 Data Complex.[18] The requirement that Apps transmit data to the PSAPs via TCC or NG9-1-1 Data Complex provides an opportunity to screen out Apps which do not comply with the standards. The fact that a small number of TCCs and NG9-1-1 Data Complexes are being deployed nationwide to serve all jurisdictions improves the practicality of such a solution.

Under BRETSA's proposal, a committee, task-force or national association would be established or designated by the Commission as the Standards Authority to consider and adopt standards for 911-related Apps, grant or deny applications for approval of Apps, and consider any requests for waiver of the adopted standards in conjunction with such applications. The Commission would bring together individuals with experience in PSAP and First Responder operations, representatives of relevant stakeholders such as originating service providers, SSPs, interest groups such as the deaf and hard of hearing community, and individuals with expertise in various disciplines appropriate to the tasks of the Authority, or assure that an entity designated as the Standards Authority included representatives of such stakeholder groups.

The Standards Authority would assign App Registration Numbers ("ARN") to Apps which it determined met the standards. These approved Apps would also be assigned codes to include in data transmission protocols which would identify to the TCCs, NG9-1-1 Data Complexes and PSAPs that the transmitted information is from an Approved App or a call center supporting an approved App. A list of approved Apps would be published by the Standards Authority, and the App developers/providers would be authorized to advertise that their App was approved by the Standards Authority. The Authority could require testing by third-party testing organizations as an application requirement or on a case-by-case basis, and take such other

[18] The NG9-1-1 Data Complex is the aggregate functions and processes required for operation of an NG9-1-1 system, including determining the location of the caller, identifying the PSAP to which the call should be delivered, routing the call to the PSAP, and cybersecurity.

measures to assure that Apps were functional, reliable and useful, and did not constitute cybersecurity risks, for example.

For such a system to be effective in assuring that Apps support rather than interfere with 9-1-1 service, regulations or statutes would be required (i) mandating that TCCs and NG9-1-1 Data Complexes delete URLs included in text-to-911 messages or other data transmissions, and (ii) deny direct interconnection with Apps which have not been approved by the Standards Committee, and with call centers associated with Apps which have not been approved. CMRS and device providers should be prohibited from including unapproved 911-related Apps in their App stores.

Statutes would also be required making it a criminal offense for an unapproved App to transmit protocols assigned to an App which *had* been approved by the Standards Authority, or to misrepresent in marketing materials that an App was approved by the Standards Authority. Misappropriation of assigned protocols or misrepresentation of approval of an App could certainly result in civil liability including for fraud. However criminal penalties should also be established because such misappropriation or misrepresentation could have dire consequences for end users, and App development does not require such significant resources as would support a presumption that providers of such Apps would not be judgment proof. Thus subjecting developers who misappropriate approved protocols or misrepresent Standards Authority approval to potential criminal prosecution is essential for deterrence.

In summary, the four parts of the recommended solution are (i) the Commission requires CMRS and device providers to publish the APIs for their native location functionalities, so that 911-related Apps can access the most reliable location data available, (ii) the Commission establishes a Standards Authority to adopt standards for 911-related Apps and approve and

publish a list of 911-related Apps which comply with the standards, (iii) the Commission adopts regulations preventing unapproved Apps from gaining access to the 911 system and CMRS and device provider App stores, and (iv) the Standards Authority recommends any legislation and/or regulation appropriate to deter providers of unapproved Apps from improperly enabling their Apps to access to the 9-1-1 system or misrepresenting the Standards Authority-approval, stakeholder endorsements, or the capabilities of their Apps or of other communications systems with respect to 9-1-1.

V. Conclusion.

Together, the issues identified by NASNA and BRETSA threaten to turn the 9-1-1 system into a "Tower of Babble," with different Apps supplying information their developers *think* is important in an emergency rather than the information public safety professionals *know* is important and critical to public safety response, and with each App formatting and organizing the information differently. Some Apps will provide data in a text-to-911 message, others will provide data through web links which may expose PSAPs to cybersecurity threats, and yet others will require the PSAP to deploy and maintain additional servers and related hardware. Some Apps will provide medical or other technical data which will be meaningless to PSAPs, because they lack the resources to employ experts in various medical, scientific and engineering fields to interpret the data. The accuracy and reliability of location information will vary from App to App. Moreover, consumers will have no guidance as to which Apps are reliable and will put them in contact with a PSAP which can dispatch First Responders to their location, and which Apps will not.

Action must be taken to avoid this result. The Commission is in the best position to commission a Standards Authority and bring together technical resources and the various

stakeholders necessary to craft a means of dealing with the burgeoning number of Apps, and preventing 9-1-1 from becoming a "Tower of Babble."

Respectfully submitted,

BOULDER REGIONAL EMERGENCY TELEPHONE SERVICE AUTHORITY

By: 

Joseph P. Benkert

Joseph P. Benkert, P.C.
P.O. Box 620308
Littleton, CO 80162
(303) 948-2200

Its Attorney

February 2, 2017